Este tutorial abarcará la configuración de una arquitectura DMZ, así como otros controles de seguridad de red.

Las DMZ son zonas desmilitarizadas, es decir, subredes diseñadas para exponer servicios externos a una red no confiable (generalmente internet). Se utilizan para proteger la red de área local (LAN) de una organización del tráfico no confiable. Visualmente, una DMZ se ubicaría entre internet y las redes privadas.

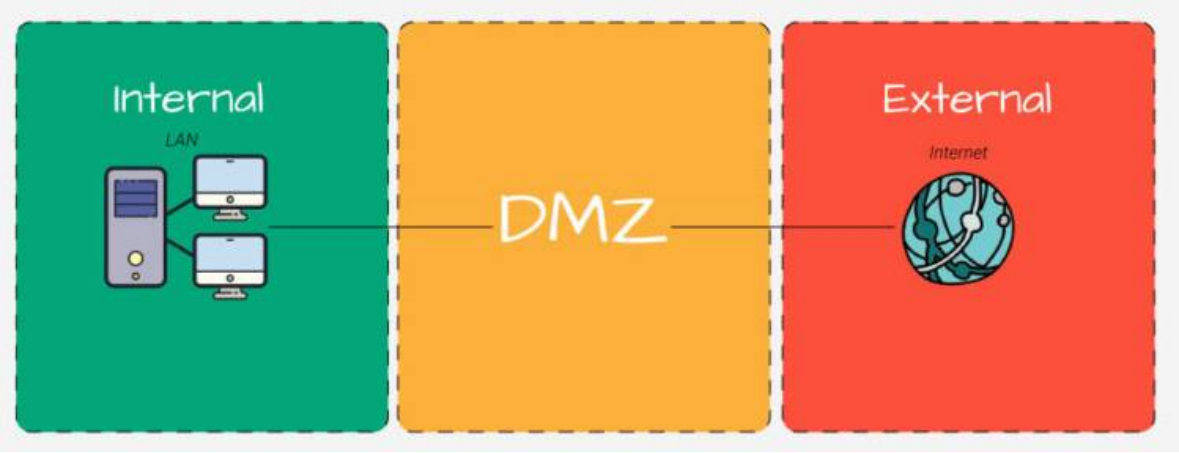
Los controles de seguridad son más eficaces cuando se integran en el sistema al que se aplican, y la infraestructura de red no es una excepción. Si bien la automatización de la red permite optimizar las configuraciones con rapidez, es más eficiente configurarlas correctamente desde el principio.

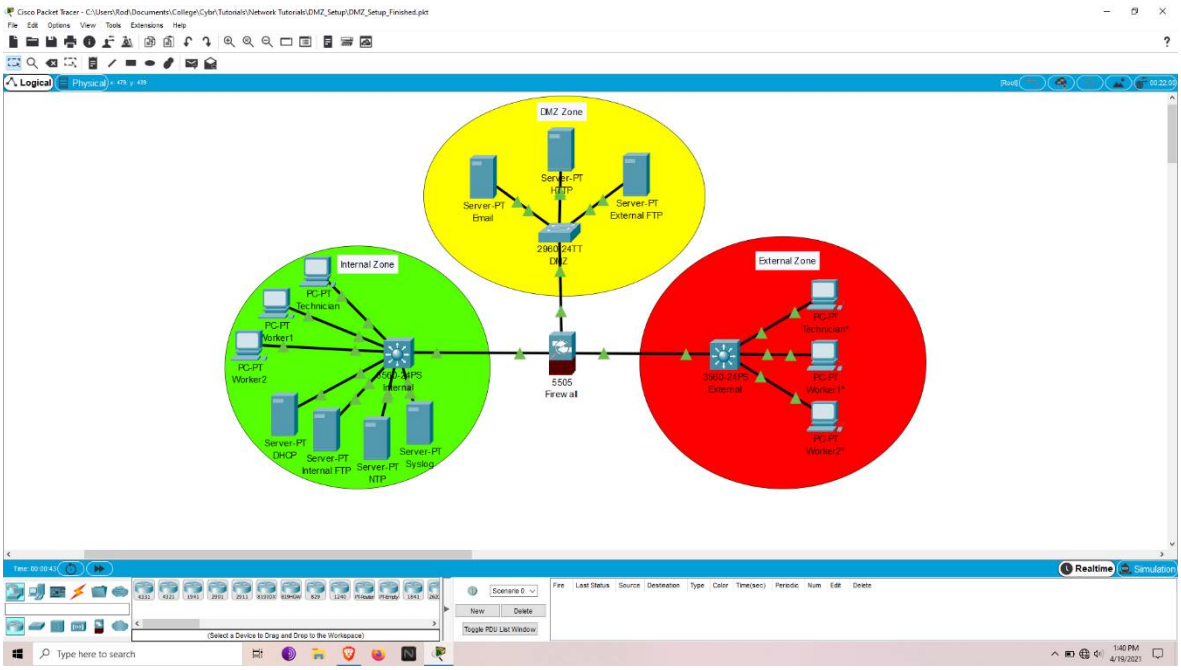
La topología consta de tres zonas principales:

Interno

Zona desmilitarizada

Externo





Considera la red interna y la DMZ como nuestra red privada. Esta estrategia de diseño es un ejemplo perfecto de cómo aumentar significativamente la seguridad mediante la segmentación de la red.

Temas a tratar:

Refuerzo de la asignación de puertos de conmutación

Configuración del servidor

Espionaje de DCHP

Inspección Arp

Configuración del firewall: configuración de la DMZ con rutas estáticas

Configuración de inicio de sesión/SSH

Listas de control de acceso (ACL)

Si algunos de estos términos le resultan desconocidos, dedique tiempo a investigarlos y, al menos, conozca su función básica en una red antes de continuar.

No se requieren conocimientos exhaustivos para al menos comenzar a configurar y ver cómo funcionan estos protocolos en la práctica.

La primera es la base sobre la que trabajar, mientras que la segunda es para que puedas ver la configuración finalizada y compararla con la tuya.

Si los dispositivos tienen contraseñas, mis valores predeterminados son:

Usuario: administrador

Contraseña: cisco

habilitar: clase

Consejos rápidos

El signo de interrogación se puede usar para cualquier parámetro posicional para ver las opciones de comando disponibles.

Ctrl + a -> Mueve el cursor al principio de la línea

Ctrl + e -> Mueve el cursor al final de la línea

Empezando

Las configuraciones básicas (entorno, VLAN, direccionamiento IP, enrutamiento estático entre VLAN) ya están configuradas, excepto el firewall.

Seguridad:

Comencemos por asignar los hosts finales a la VLAN apropiada y proteger las interfaces físicas.

El diseño de VLAN es relativamente simple, con VLAN para trabajadores, técnicos y VLAN separadas para los distintos servidores.

Esto ayuda a crear segmentación, así como control de acceso cuando se aplican ACL.

Mi estrategia recomendada es configurar los puertos troncales y de acceso en rangos separados. Asegúrese de configurar todos los comandos uniformes que se aplican a todas las interfaces en ese rango; luego, aplique comandos específicos de interfaz como `switchport access vlan [vlan #]`.

Un enfoque ideal:

Asigna los puertos no utilizados a la VLAN Black_Hole y desactívalos.

Seleccione todas las interfaces de acceso y asígneles comandos uniformes.

Asignar interfaces correspondientes a las VLAN.

CONFIGURACIONES PASO A PASO

INTERNAL:

conf t

int ran f0/4-19, g0/1-2

switchport access vlan 999

shut

int ran f0/1-23, g0/1-2

switchport mode access

switchport port-security

switchport port-security mac-address sticky

int f0/1

switchport access vlan 20

int ran f0/2-3

switchport access vlan 10

int f0/20

switchport access vlan 30

int f0/21

switchport access vlan 40

int ran f0/22-23

switchport access vlan 50

end

wr

EXTERNAL:

conf t

int ran f0/4-23, g0/1-2

switchport access vlan 999

shut

int ran f0/1-23, g0/1-2

switchport mode access

switchport port-security

switchport port-security mac-address sticky

int f0/1

switchport access vlan 80

int ran f0/2-3

switchport access vlan 70

end

wr

DMZ:

conf t

int ran f0/4-23, g0/1-2

switchport access vlan 999

shut

int ran f0/1-23, g0/1-2

switchport mode access

switchport port-security

switchport port-security mac-address sticky

int ran f0/1-3, f0/24

switchport access vlan 50

end

wr

Verifica configuraciones:

show run

show ip interface brief

show vlan brief

show port security

Configuración interna del servidor.

Para configurar servidores en Packet Tracer, simplemente abra el servidor y haga clic en la pestaña de servicios.

Tenga en cuenta que todos los servicios no utilizados están desactivados.

Antes de configurar cualquiera de estos servicios, asegúrese de que estén activados.

DHCP

Ahora configuremos DHCP para asignar dinámicamente direcciones IP a los hosts finales.

La asignación de direcciones DHCP se determina mediante la tabla IP. Agreguemos un grupo de direcciones para cada VLAN.

En el servidor DHCP:

Haz clic en la pestaña de servicios, ve a DHCP y completa el siguiente formato:

Pool Name	**Default Gateway**	**Start IP**	**Subnet Mask**	**Max User**
serverPool	0.0.0.0	192.168.30.0	255.255.255.252	0
Worker Pool	192.168.10.1	192.168.10.2	255.255.255.248	2
Technician Pool	192.168.20.1	192.168.20.2	255.255.255.252	1

INTERNAL:

conf t

int vlan 10

ip helper-address 192.168.30.2

int vlan 20

ip helper-address 192.168.30.2

end

wr

En este punto, DHCP debería ser configurable en los hosts finales. Simplemente haga clic en los hosts finales, haga clic en la pestaña de configuración y seleccione FastEthernet0 o haga clic en la pestaña de escritorio y configuración de IP; luego cambie de IP estática a DHCP.

Para conexiones externas, se configurará en el switch L3 en lugar de en un servidor, lo cual es notablemente similar a la configuración DHCP de un router.

EXTERNAL:

conf t

ip dhcp excluded-address 10.0.70.1

ip dhcp excluded-address 10.0.80.1

ip dhcp pool WORKERS

network 10.0.70.0 255.255.255.248

default-router 10.0.70.1

ip dhcp pool TECHNICIAN

network 10.0.80.0 255.255.255.252

default-router 10.0.80.1

end

wr

Verifica las configuraciones:

sh run

sh ip dhcp binding

sh ip dhcp pool

Ahora los hosts externos están listos para que se les asignen direcciones IP.

FTP INTERNAL

Primero abre el servidor FTP, elimina el nombre de usuario predeterminado y utiliza la siguiente estructura:

Username	Password	Permission
admin	cisco	RWDNL
user	cisco	RL

Obviamente, en un escenario real, deberían utilizarse contraseñas mucho más seguras.

Por el momento, ignoremos la seguridad de las contraseñas y centrémonos en los protocolos.

Verificar configuraciones

Abra el símbolo del sistema en un host final de la zona interna.

Ejecutar comandoftp 192.168.40.2

Proporcione el usuario y la contraseña (admin, cisco)

Corre dira ver qué hay disponible.

Ejecutar get [name of file]para recuperar un archivo

NTP y Syslog

NTP y Syslog se configurarán en la red interna, lo que proporcionará capacidad de auditoría de registros.

NTP sincronizará los relojes del sistema de los dispositivos de red en la red privada.

Syslog utilizará NTP para facilitar el envío de mensajes de registro a un servidor para todos los dispositivos de la red privada.

NTP debe configurarse primero, ya que Syslog sería inútil sin él.

En el servidor NTP:

Habilitar autenticación

Clave: 1

Contraseña: cisco

En el servidor Syslog:

Confirmo que el servicio está activado

INTERNAL:

Normalmente es necesario configurar las marcas de tiempo, pero eso ya se ha tenido en cuenta en las configuraciones básicas de todos los dispositivos.

No es necesario configurar nada, pero aquí están los comandos como referencia:

service timestamps log datetime msec

service timestamps debug datetime msec

Ahora, ¿qué queda por hacer?

conf t

ntp server 192.168.50.2

ntp authenticate

ntp authentication-key 1 md5 cisco

ntp trusted-key 1

ntp update-calendar

logging 192.168.50.3

logging on

logging userinfo

logging trap

end

wr

Verificar configuraciones:

show clock

show ntp associations

show ntp status

show logging

Configuración de servidor externo

Correo electrónico

En la pestaña de servicios, confirme que el servicio de correo electrónico está activado, configure el nombre de dominio internal.nety agregue lo siguiente:

Contraseña de usuario

Administrador de Cisco

Usuario de Cisco

Verificar configuraciones

Enviar un correo electrónico

HTTP

Confirme que el servicio está habilitado para http/https.

Verificar configuraciones:

Abra un navegador en un host final en zonas internas o externas y conéctese a http://172.16.50.4

FTP externo

Consulte la configuración FTP interna anterior.

Verificar configuraciones:

El mismo método que para FTP interno.

Antes de pasar a configurar la DMZ, establezcamos algunos controles de seguridad LAN de capa 2 adicionales.

Inspección DHCP

Esta función supervisa y facilita los mensajes para un servidor DHCP. Ayuda a identificar anomalías en el proceso de solicitud DHCP DORA (Descubrimiento, Oferta, Solicitud, Confirmación) y descarta las solicitudes incorrectas.

Esto impide que los atacantes modifiquen el tráfico DHCP para manipular sus capacidades dinámicas y obtener acceso a la red.

Los únicos puertos que deben ser de confianza son las conexiones desde el switch al servidor DHCP y las conexiones entre switches.

INTERNAL:

conf t

ip dhcp snooping

ip dhcp snooping vlan 10,20

ip dhcp snooping verify mac-address

int f0/20

ip dhcp snooping trust

ip dhcp snooping limit rate 100

int ran f0/1-19, f0/21-23, g0/1-2

ip dhcp snooping limit rate 20

end

wr

La configuración anterior no solo establece el puerto del servidor como de confianza, sino que también limita la tasa de tráfico DHCP permitido a través de las interfaces.

EXTERNAL:

conf t

ip dhcp snooping

ip dhcp snooping vlan 70,80

ip dhcp snooping verify mac-address

int ran f0/1-23, g0/1-2

ip dhcp snooping limit rate 20

end

wr

Verificar configuraciones:

sh ip dhcp snooping

ARP Inspection

Esta función es similar a DHCP Snooping y depende de él, pero en lugar de eso, supervisa el tráfico ARP.

Para quienes no estén familiarizados, ARP (Protocolo de Resolución de Direcciones) se utiliza para consultar al switch la dirección IP de capa 3 basándose en la tabla MAC. Se le conoce comúnmente como un protocolo de mapeo de direcciones de capa 2 a capa 3.

Sin ARP, DHCP asignaría una dirección, pero el host no sabría cómo salir de la red interna a internet. La inspección ARP evita las solicitudes ARP innecesarias, que se solicitan manualmente en lugar de ser el resultado del proceso DHCP DORA.

Esto evita la modificación de solicitudes y protege la tabla ARP de posibles errores. Los paquetes con enlaces MAC a IP no válidos se descartarán.

INTERNAL:

conf t

ip arp inspection vlan 10,20

ip arp inspection validate src-mac

end

wr

EXTERNAL:

conf t

ip arp inspection vlan 70,80

ip arp inspection validate src-mac

end

wr

También se puede configurar el límite de velocidad, al igual que con DHCP Snooping. Por defecto es 15, lo cual es adecuado para esta red.

Verificar configuraciones:

sh ip dhcp snooping

Configuración del firewall DMZ

Ahora, finalmente, ha llegado el momento de conectar la DMZ con la zona interna configurando el firewall ASA.

El primer paso es eliminar cualquier configuración predeterminada no deseada y, a continuación, configurar el resto.

El firewall modelo es un Cisco ASA 5505, que opera en una configuración VLAN de capa 2, por lo que se requiere una SVI (Interfaz Virtual de Switch) para la asignación de IP (como un switch de capa 3).

FIREWALL ASA CISCO

conf t

no dhcpd enable inside

no dhcpd address 192.168.1.5-192.168.1.36 inside

no dhcpd auto_config outside

telnet timeout 1

int vlan 1

ip addr 192.168.1.2 255.255.255.252

int vlan 2

nameif dmz

ip addr 172.16.50.1 255.255.255.248

security-level 70

no forward interface vlan 1

int vlan 3

nameif outside

ip addr 209.165.200.2 255.255.255.252

int vlan 4

exit

route inside 192.168.0.0 255.255.0.0 192.168.1.1

route outside 0.0.0.0 0.0.0.0 209.165.200.1

object network inside-net

subnet 192.168.0.0 255.255.0.0

nat (inside,outside) dynamic interface

int e0/0

switchport access vlan 1

no shut

int e0/1

switchport access vlan 2

no shut

int e0/2

switchport access vlan 3

no shut

int e0/3

switchport access vlan 4

shut

int e0/4

switchport access vlan 4

shut

int e0/5

switchport access vlan 4

shut

int e0/6

switchport access vlan 4

shut

int e0/7

switchport access vlan 4

shut

```
exit
class-map CMAP
match default-inspection-traffic
exit
policy-map PMAP
class CMAP
inspect dns
inspect ftp
inspect http
inspect icmp
exit
service-policy PMAP global
end
write memory
```

La configuración anterior elimina los valores predeterminados no deseados, configura las interfaces SVI (con `black_hole` para las interfaces no utilizadas), las asigna a un puerto de switch y deshabilita las interfaces no utilizadas (el firewall de Packet Tracer, lamentablemente, no incluye rangos de interfaces de acceso). A continuación, crea un mapa de clases que se vincula a un mapa de políticas, el cual, finalmente, se vincula a la política de servicio global.

En este punto, la zona interna debería poder comunicarse con cualquier zona, mientras que la DMZ y la zona externa pueden comunicarse entre sí, pero están aisladas de la zona interna.

Resulta bastante obvio por qué este es un enfoque ideal para una arquitectura segura, aunque dista mucho de ser infalible.

Un bloque de JavaScript o ejecutables bien diseñados, iniciados a través de sitios web, correos electrónicos, etc., aún podrían lograr infiltrarse. Esto puede infectar la sesión del usuario, lo que permite que su tráfico se mezcle con el flujo de datos para eludir el firewall. De esta forma, el ataque parece formar parte de una conexión saliente permitida, en lugar de intentar infiltrarse con una conexión entrante propia.

Por eso, la formación de los usuarios finales es uno de los aspectos más críticos de la superficie de ataque. La falta de comprensión puede dar lugar a actividades que tienen el potencial de eludir las distintas capas de controles de seguridad.

Verificar configuraciones:

sh run

sh ip

sh int ip br

sh nat

sh route

Inicio de sesión/SSH

Normalmente, para redes más grandes, recomendaría utilizar AAA para la autenticación remota y usar la autenticación local como respaldo en caso de que falle el servidor remoto.

Dado que solo vamos a reforzar la seguridad de 3 dispositivos, no es motivo de gran preocupación. Si se produjeran problemas de conectividad, de todas formas habría que acceder a ellos físicamente.

INTERNAL y la DMZ:

conf t

username admin privilege 15 secret cisco

enable secret class

login block-for 300 attempts 5 within 120 # <= Login commands unavailable on DMZ L2 switch

login on-success log

login on-failure log

crypto key generate rsa # <= hit enter, select biggest key size, hit enter again (Firewall already has key-pair)

line con 0

privilege level 15

login local

exit

line vty 0 15

privilege level 15

login local

end

wr

FIREWALL

conf t

username admin password ciscoasapassword encrypted

enable password class

ssh 192.168.20.2 255.255.255.255 inside

crypto key generate rsa modulus 2048 # <= answer yes when prompted

end

write memory

Verificar configuraciones:

sh run

sh login

sh ip ssh

A pesar de la configuración, es posible que SSH siga sin funcionar en el ASA con Packet Tracer. Se trata de una función relativamente nueva que aún presenta algunos errores y está menos desarrollada que la de los routers y switches.

Aunque no está disponible en Packet Tracer, recomiendo deshabilitar telnet y forzar el uso exclusivo de ssh.

Listas de control de acceso (ACL)

Ahora, trabajemos en la zona interna como una segunda capa de protección en caso de que se vulnere el firewall, para aislar las VLAN internas según el control de acceso de mínimo privilegio y para proteger las capacidades de acceso remoto de las líneas VTY de nuestros dispositivos de red.

INTERNAL:

conf t

ip access-list standard SyslogNTP

deny any

exit

int vlan 50

ip access-group SyslogNTP in

exit

end

ip access-list extended SSH

permit tcp host 192.168.20.2 any eq 22

exit

line vty 0 15

access-class SSH in

wr

Lenguaje de programación: PHP (php)

Verificar configuraciones:

sh run

sh access-lists

La configuración anterior establece que la VLAN NTP/Syslog sea inaccesible para los usuarios finales y que el inicio de sesión SSH solo esté disponible para el técnico.

Conclusión

En este tutorial hemos abarcado muchos temas, pero espero que hayan disfrutado siguiéndolo y configurando su red. Ahora, pueden experimentar con pruebas de ping y traceroute en el entorno, probando diferentes combinaciones de zonas para ver qué funciona y qué no.

ING. PABLO PALACIOS

2025
